Research on System Structure of Mobile Internet Security Audit

Xia-Meng Si, School of Software Engineering, Beijing University of Posts and Telecommunications. Beijing, China

ABSTRACT

As the development of mobile internet bring convenient for people, the openness and variety of services make its security issues more complicated than those of traditional network. Firewall and intrusion detection focuses on external aggression, and cannot prevent revealing of internal information. As supplementary, security audit technology can monitor internal users’ activity, forbid abnormal behavior of internal users. The author introduces related works about mobile internet security audit, comb through matured products on the market, and analyze current security status and architecture of mobile internet security. Based on the research results of traditional network security audit, the author provides a functional framework and universal model of mobile internet security auditing, as well as introduce an application scenario.

KEYWORDS

Mobile Internet, Network Security, Security Audit, Security Incident

1. INTRODUCTION

With the rapid development of mobile network and internet technology, the influences of mobile internet on people’s daily life have already infiltrated the financial, trade, transportation, education and other fields. At the same time, the diversity of mobile internet business applications, the openness of the wireless communication and the limited computing power of mobile terminal, these objective reasons lead to wanton spread of bad information, mobile internet virus, network security problem such as illegal access are far more difficult than the security problem of traditional network.

At present, the more popular security technologies such as firewall (Bulbul, Sapkota, Ten, Wang, Ginter, 2015), intrusion detection (Tuck, Sherwood, Calder, Varghese, 2004), these traditional technology are mainly for the network or the external attack defense and detection of system, but for the internal information security of network or system (such as information leakage, after leaving marks, etc.) threat to do. Security audit technique can audit and control behavior online, track behavior real-time, and confirm the necessary records which are documented; it can audit and control the outgoing data content of mobile terminals to prevent the leakage of audit domain data; it also can prevent the mobile internet abuse and increase the service efficiency of the network. Mobile internet security audit technology is used for monitoring the behavior of the mobile internet in mobile terminal access to the internal and external network data, and it plays an important role to prevent internal mobile terminal attacks and misuse of network, it also can effectively achieve the safety supervision of internal network, protect sensitive information stored in the mobile terminal, and solve the problem of a mobile user which is difficult to source. It provides evidence base for the mobile internet safety accident treatment and irregularities traceability.

Mobile internet security audit, which realizes monitor, collect information, and analysis the various events and behavior of the mobile internet, and take the appropriate response actions to specific events and behavior. This paper analyzes the present situation and framework of the mobile internet, and points out that the positions of the security audit in the mobile internet security system.
It puts forward the functional framework and universal model of the mobile internet security audit, and introduces a kind application scenario of mobile internet security audit technology application scenario.

2. THE PRESENT RESEARCH

At present, the security audit technology and products which is aim at the traditional network relatively mature. The research and application of mobile internet security audit is also gradually aroused widespread attention, but it is still in its infancy, the security audit products on the market are relatively small.

Technology research, depending on the difference of audit target, audit contents, audit methods and techniques, probably there are the safety audit based on the log, based on the Network traffic, based on the data mining and so on. Literature (Wang, Liu, Hu, Jiang, 2013) puts forward a kind of effective audit method for network security based on agent and log mining technology, improve the traditional rules mining algorithm Apriori and design a new data structure, which makes the audit system scans the database only once and has obvious advantages than Apriori algorithm on system I/O cost.

Literature (Huang, & Sheu, 2007) proposes a distributed multi-layer security audit system based on data mining technology, using the XML log format, keyword matching, fuzzy clustering technology and related safety rules. The detection efficiency and the ability to discover unknown attacks were improved. With the wide application of cloud computing, virtualization and multiple lease makes the network structure is more complex, the service, which brought difficulties for monitoring, backup, restore, especially safety management. Based on this, Doelitzscher puts forward a new cloud auditing standards and a set of cloud security audit system (Doelitzscher, 2014), which is able to provide flexible security audit functions in changing cloud network, and also designs a cloud audit policy language. Considering the existing security auditing system only can monitor internal LAN, and can’t realize the real-time and continuous auditing for the characteristics of cross-regional, cross segment of mobile internet devices. Literature (Zhang, Xu, Zhao, Wang, 2014) proposed a security audit framework for mobile internet equipment, using the embedded intelligent probe technique and data from technology, combined with the existing cloud and big data processing platform, puts forward the cross-regional mobile internet audit cloud which is also across a network segment, realize the mobile internet devices of cross-regional, across the security audit. This architecture can take full advantage of the powerful computing resources and storage resources that cloud platform provides, Centralized store, manage and analysis the audit data distributed in different regions and segments, realize the quickly position for the mobile terminal existing problems.

In respect of products, there have been some excellent security audit products at home and abroad in recent years. But due to the particularity of network security audit, which required security vendor must support for local application. Such as the limitation for IM (Instant Messaging) software, the foreign audit system focused on ICQ, MSN, Skype, etc., and domestic concerns that tencent QQ, micro letter, taobao wangwang, etc., therefore, foreign security auditing system does not apply to the domestic actual situation to a great extent. Main domestic security audit products provider typically have Hanbang, Venus, Topsec, Inspur, Nsfocus, Fudan Guanghua, Xianjiaoda jump, Zhongke emerging net. Early products are mainly for the traditional internet. In recent years, the development and upgrading of the mobile internet has been carried out, and began to launch practical products. The audit information comprehensive security monitoring system of Hanbangruanke (http://wenku.baidu.com/link?url=SfOc2hl0hB-xo9PhjQfXPLehmBggLajf1fV54AW39sk0cJ8_AgCce1_6hb6Lx5aQCF4_A9Q_ZbSUGJJeBBs5KWfeWQ_vDrQcMdpvdWD3Ifnba) is composed of three parts, the audit center, the host sensor, and the network engine. Its main functions are: the internal and external supervision, the network behavior audit, the host authority management, database operation audit, etc. Comprehensive security audit system of talent (http://down.51cto.com/data/1159873) collects the information of all kinds of network resources and System log information, provides a unified centralized management.
Green Cognitive Relay Communications with Hardware Impairments for Future Wireless Networks

Asymmetric Geographic Forwarding: Exploiting Link Asymmetry in Location Aware Routing

Simulating Realistic Urban Scenarios for Ad Hoc Networks